UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/626,948	07/25/2003	Anne Kirsten Eisentraeger	MS1-1276US	3219

22801 7590 11/17/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/626,948	EISENTRAEGER ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-72* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-72* is/are rejected.

7)☒ Claim(s) *5-15, 19-26, 30-37,43-46, 49, 52, 58-63, 67-68 and 71-72* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/22/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-72** have been examined.

Priority

2. This application does not claim priority of an application. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **07/25/2003.**

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. **Independent Claims 1, 16, 27, 38, 47, 50, 53-56, 65 and 69** are rejected under 35 U.S.C. 101 because the subject matter is directed to non-statutory subject matter.

5. **Claims 1, 16, 27, 53-56, 65 and 69** are directed to a method comprising, selecting an elliptic curve; determining a Squared Weil pairing based on said elliptic curve; and **cryptographically processing selected information based on said Squared Weil pairing**. The examiner asserts that the limitation of the claims does not fall within the statutory classes listed in 35 USC 101. The language of the claims, **"cryptographically processing selected information based on said Squared Weil pairing"** raises a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result

in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101. See MPEP § 2106 IV. B. 1(a). As indicated on paragraph 0061, of the applicant publication 2005/0036609 A1, the above recited limitation is a particular algorithm, and algorithm per se is not statutory unless it is tied to a technological art, environment or machine that would result in a practical application **producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101**.

6. **Independent claims 38, 47 and 50** are directed to a method comprising, determining a Squared Well Pairing by: establishing an odd prime m on a curve E; and based on two m-torsion points P and Q on E, computing $e_m(P, Q)^2$. The examiner asserts that the limitation of the claims does not fall within the statutory classes listed in 35 USC 101. The language of the claims, "**based on two m-torsion points P and Q on E, computing $e_m(P, Q)^2$**" raises a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application **producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101**. See MPEP § 2106 IV. B. 1(a). As indicated on paragraph 0061, of the applicant publication 2005/0036609 A1, the above recited limitation is a particular algorithm, and algorithm per se is not statutory unless it is tied to a technological art, environment or machine that would result in a practical application **producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101**.

7. **Dependent claims 2-15, 17-26, 28-37, 39-46, 48-49, 51-52, 57-64, 66-68 and 70-72** are also rejected under 35 U.S.C. 101 because the subject matter is directed to non-statutory subject matter and for the same reasons as that of the corresponding independent claims.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. **Claims 1-4, 16-18, 27-29,56-57, 64, 65-66 and 69-70** are rejected under 35 U.S.C. 102(e) as being anticipated by **Boneh et al**(hereinafter refereed as **Boneh**) (U.S. Patent Publication No. 2003/0081785A1) (Filed on August 13, 2002)(Claims priority of provisional application 60/311,946, filed on August 13, 2001)

10. **As per claims 1, 16, 27, 56-57, 64-65 and 69 Boneh discloses** a method comprising: selecting an elliptic curve; determining a Squared Weil pairing based on said elliptic curve; and cryptographically processing selected information based on said Squared Weil pairing. [Abstract, paragraph 0331-0347, paragraph 0354-0357] (As it is disclosed on the abstract, According to one embodiment, the bilinear map is based on a **Weil pairing or a Tate pairing defined on a subgroup of an elliptic curve**. Furthermore on paragraph 0331-0347, how the weil pairing is computed is disclosed on paragraph 0354, "To evaluate the Weil pairing e(P, Q), how the **repeated squaring algorithm** needs evaluate a function is also disclosed.)

11. **As per claims 2, 17, 28, 57, 66 and 70 Boneh discloses** a method as applied to claim above. Furthermore, Boneh discloses the method wherein, said elliptic curve

includes an elliptic curve E over a field K, wherein E can be represented as an equation $y^2 = x^3 + ax + b$. [paragraph 0308]

12. **As per claims 3-4, 18 and 29, Boneh discloses** a method as applied to claim above. Furthermore, Boneh discloses the method wherein, determining said Squared Well pairing based on said elliptic curve further includes establishing a point id that is defined as a point at infinity on E, and wherein P, Q, R, X are points on E wherein X is an indeterminate denoting an independent variable of a function, and wherein x(X), y(X) are functions mapping said point X on E to its affine x and y coordinates, and wherein a line passes through said points P, Q, R if P+Q+R=id. [Paragraph 0316 and 0335-0357]

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. **Claims 38-41, 47-48 and 50-51** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Boneh et al**(hereinafter refereed as **Boneh**) (U.S. Patent Publication No. 2003/0081785A1) (Filed on August 13, 2002)(Claims priority of provisional application 60/311,946, filed on August 13, 2001) in view of Ellis **J. Manoharmayum** (hereinafter refereed as **Mano**) (Mathematical Research, Letters) (January 23, 2001)(Revised Version August 29, 2001) (Reference U)

15. **Claims per claims 38-41, 47-48 and 50-51 Boneh discloses** a method comprising: selecting an elliptic curve; determining a Squared Weil pairing based on said elliptic curve; and cryptographically processing selected information based on said

Squared Weil pairing. [Abstract, paragraph 0331-0347, paragraph 0354-0357] (As it is disclosed on the abstract, According to one embodiment, the bilinear map is based on a **Weil pairing or a Tate pairing defined on a subgroup of an elliptic curve**. Furthermore on paragraph 0331-0347, how the weil pairing is computed is disclosed on paragraph 0354, "To evaluate the Weil pairing e(P, Q), how the **repeated squaring algorithm** needs evaluate a function is also disclosed.)

Boneh does not explicitly disclose determining/computing a Squared Weil Pairing $e_m(P, Q)^2$ by:

establishing an odd prime m on a curve E; and based on two m-torsion points P and Q on E.

However, in the same field of endeavor **Mano**, discloses

- establishing an odd prime m on a curve E; and based on two m-torsion points P and Q on E. [page 707, 1st paragraph, page 704, 2nd paragraph, last line and 3rd paragraph, under the title "A result of skinner and Wiles]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of establishing an odd prime m on a curve E; and based on two m-torsion points P and Q on E,as per teachings of **Mano**, into the method taught by **Boneh** in order to provide an efficient elliptic curves with potentially multiplicative reduction. [See **Mano** page 711, last 2 paragraph]

16. **Claim 42** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Boneh et al**(hereinafter refereed as **Boneh**) (U.S. Patent Publication No. 2003/0081785A1) (Filed on August 13, 2002)(Claims priority of provisional application 60/311,946, filed on August 13, 2001) in view of Ellis **J. Manoharmayum** (hereinafter refereed as **Mano**) (Mathematical Research, Letters) (January 23, 2001)(Revised Version August 29, 2001)

(Reference U) further in view of IEEE, Transactions on information theory vol 45, no. 5, July 1999. (pages 1717-1719) (hereinafter refereed as **IEEE)** (Reference V)

17. **Claims per claim 42 Boneh discloses** a method comprising: selecting an elliptic curve; determining a Squared Weil pairing based on said elliptic curve; and cryptographically processing selected information based on said Squared Weil pairing. [Abstract, paragraph 0331-0347, paragraph 0354-0357] (As it is disclosed on the abstract, According to one embodiment, the bilinear map is based on a **Weil pairing or a Tate pairing defined on a subgroup of an elliptic curve**. Furthermore on paragraph 0331-0347, how the weil pairing is computed is disclosed on paragraph 0354, "To evaluate the Weil pairing e(P, Q), how the **repeated squaring algorithm** needs evaluate a function is also disclosed.)

Boneh does not explicitly disclose determining/computing a Squared Weil Pairing $e_m(P, Q)^2$ by:

establishing an odd prime m on a curve E; and based on two m-torsion points P and Q on E.

However, in the same field of endeavor **Mano**, discloses

- establishing an odd prime m on a curve E; and based on two m-torsion points P and Q on E. [page 707, 1st paragraph, page 704, 2nd paragraph, last line and 3rd paragraph, under the title "A result of skinner and Wiles]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of establishing an odd prime m on a curve E; and based on two m-torsion points P and Q on E, as per teachings of **Mano,** into the method taught by **Boneh** in order to provide an efficient elliptic curves with potentially multiplicative reduction. [See Mano, page 711, last 2 paragraph]

The combination of **Mano and Boneh** does not disclose that the mathematical chain has a length O(log(m)).

However, in the same field of endeavor, IEEE, discloses that the mathematical chain has a length O(log(m)).[see page 1718, 2nd column, paragraph 6]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature of adding time complexity of the chain as per teachings of IEEE into the method taught by the combination of **Mano and Boneh** in order to determine the computational **complexity of the method.**

Allowable Subject Matter

18. **Claims 5-15, 19-26, 30-37, 43-46, 49, 52, 58-63, 67-68 and 71-72** objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

19. **Claims 53-55** would be allowable if rewritten to overcome the §101 rejection set forth in this office action.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax

phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
10/28/2006

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100